Operating System

Active Directory Overview

White Paper

Abstract

The Active Directory™ service is a central component of the Windows® 2000 operating system platform. Understanding Active Directory is important to understanding the overall value of Windows 2000. This introduction to the concepts and technologies behind Active Directory describes its purpose, provides an overview of how it works, and outlines the key business and technical benefits it offers organizations.

© 2000 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, the BackOffice logo, Visual Basic, , Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0798

CONTENTS

INTRODUCTION.....1

WHY HAVE A DIRECTORY SERVICE?.....2

WHAT IS ACTIVE DIRECTORY?.....3

THE MICROSOFT DIRECTORY SERVICE STRATEGY.....4

HOW DOES ACTIVE DIRECTORY WORK?.....5
Hierarchical Organization 5
Object-oriented Storage 5
Multi-Master Replication 6

WHAT ARE THE BENEFITS OF ACTIVE DIRECTORY?.....8
Simplifies Management 8
How Active Directory Simplifies Management 8
Strengthens Security 9
How Active Directory Strengthens Security 10
Extends Interoperability 11
How Active Directory Extends Interoperability 11

Conclusion.....13

WHAT HAVE TO DIRECTORY SERVICE?

The Active Directory™ service is a central component of the Windows® 2000 operating system platform. Understanding Active Directory is important to understanding the overall value of Windows 2000. This introduction to the concepts and technologies behind Active Directory describes its purpose, provides an overview of how it works, and outlines the key business and technical benefits it offers organizations.

Today, networked computing is more important than ever for businesses to remain competitive. As a result, modern operating systems require mechanisms for managing the identities and relationships of the distributed resources that make up network environments. A directory service provides a place to store information about network-based entities, such as applications, files, printers, and people. It provides a consistent way to name, describe, locate, access, manage, and secure information about these individual resources.

Further, a directory service acts as the main switchboard of the network operating system. It is the central authority that manages the identities and brokers the relationships between these distributed resources, enabling them to work together. Because a directory service supplies these fundamental network operating system functions, it must be tightly coupled with the management and security mechanisms of the operating system to ensure the integrity and privacy of the network. It also plays a critical role in an organization's ability to define and maintain the network infrastructure, perform system administration, and control the overall user experience of a company’s information systems.

The need for an ever more powerful, transparent, and tightly integrated directory service is driven by the explosive growth of networked computing. As local area networks (LANs) and wide area networks (WANs) grow larger and more complex, as networks are connected to the Internet, and as applications require more from the network and are linked to other systems through corporate intranets, more is required from a directory service. A directory service is one of the most important components of an extended computer system because it:

- **Simplifies management.** Provides a single, consistent point of management for users, applications, and devices.
- **Strengthens security.** Provides users with a single sign-on to network resources and provides administrators with powerful and consistent tools to manage security services for internal desktop users, remote dial-up users, and external e-commerce customers.
- **Extends interoperability.** Supplies standards-based access to all Active Directory features as well as synchronization support for

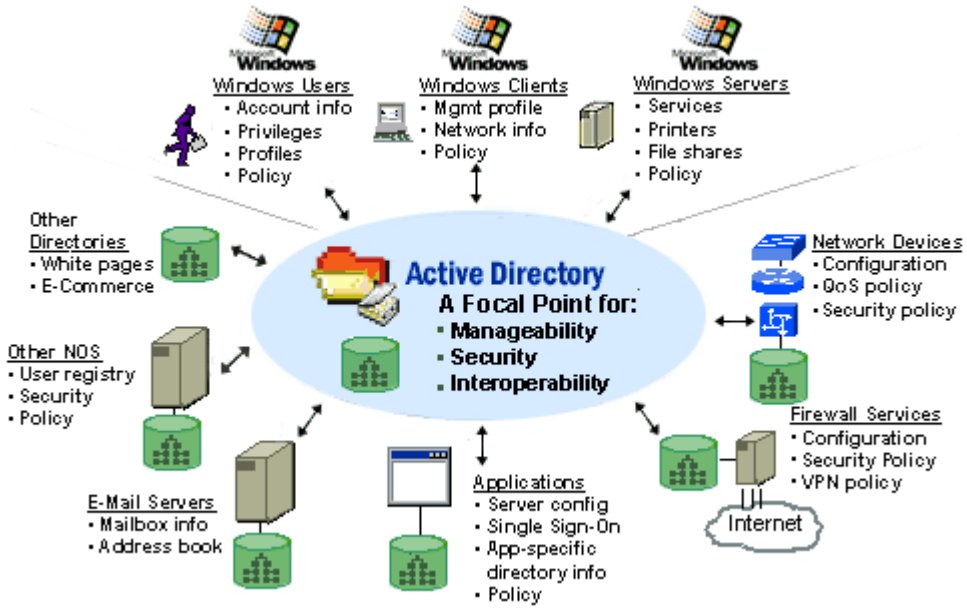
WHAT IS ACTIVE DIRECTORY?

popular directories.

A directory service is both a management and user tool. As the number of objects in a network grows, the directory service becomes essential. The directory service is the hub around which a large distributed system turns. To address these needs, Windows 2000 Server introduces Active Directory, an integrated set of directory services that improve the management, security, and interoperability of the Windows network operating system.

Active Directory is an essential and inseparable part of the Windows 2000 network architecture that improves on the domain architecture of the Windows NT® 4.0 operating system to provide a directory service designed for distributed networking environments. Active Directory lets organizations efficiently share and manage information about network resources and users. In addition, Active Directory acts as the central authority for network security, letting the operating system readily verify a user's identity and control his or her access to network resources. Equally important, Active Directory acts as an integration point for bringing systems together and consolidating management tasks.

Combined, these capabilities let organizations apply standardized business rules to distributed applications and network resources, without requiring administrators to maintain a variety of specialized directories.



Active Directory provides a single point of management for Windows-based user accounts, clients, servers, and applications. It also helps organizations integrate systems not using Windows with Windows-based

applications, and Windows-compatible devices, thus consolidating directories and easing management of the entire network operating system. Companies can also use Active Directory to extend systems securely to the Internet. Active Directory thus increases the value of an organization's existing network investments and lowers the overall costs of computing by making the Windows network operating system more manageable, secure, and interoperable.

Many vendors build specialized repositories or directory services into their applications and devices to enable the specific functionality their customers require. For example, e-mail products include directory services that let users look up and send mail to others. And server operating systems use directory services for features such as user account management and storing configuration information about applications. Because these directory services are targeted narrowly to the needs of the application or device and often lack standards-based interfaces, most companies have found that they are responsible for many different directories that can't be managed centrally or interoperate easily with each other. Having many incompatible directory services means that:

- End users must use multiple user accounts and passwords to log in to different systems, and they must know the exact locations of information on the network.
- Administrators must understand how to manage each directory within the network and must duplicate many steps when procedures, such as adding a new employee to a company, involve many different directories.
- Application developers must write different logic for every directory that their applications need to access.

The proliferation of customized directory services translates directly into a continually rising cost of ownership: it requires greater management, necessitates more complex applications, and adversely affects the productivity of the end user. In the near term, companies need to find ways to halt this trend and minimize the total number of directories that they have through proactive consolidation. Over the longer term, the best solution is to standardize based on technologies that provide the required levels of scalability, standards-based interoperability, and operating system integration.

Active Directory is the first enterprise-class directory service that is scalable, built from the ground up using Internet-standard technologies, and fully integrated with the operating system. In addition to providing

HOW DOES ACTIVE DIRECTORY WORK?

comprehensive directory services to Windows applications, Active Directory is designed to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies have. This makes Active Directory the ideal long-term foundation for corporate information-sharing and common management of network resources, including applications, network operating systems, and directory-enabled devices.

The following section gives an overview of the core Active Directory technologies.

Active Directory lets organizations store information in a hierarchical, object-oriented fashion, and provides multi-master replication to support distributed network environments.

Hierarchical Organization

Active Directory uses objects to represent network resources such as users, groups, machines, devices, and applications. It uses containers to represent organizations, such as the marketing department, or collections of related objects, such as printers. It organizes information in a tree structure made up of these objects and containers, similar to the way the Windows operating system uses folders and files to organize information on a computer.

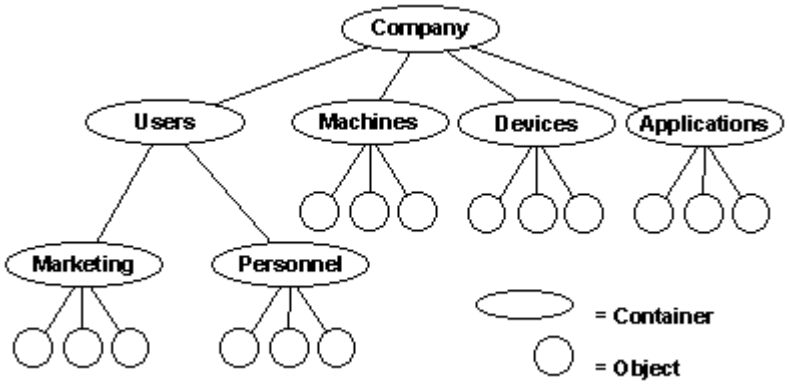


Figure 1: Active Directory organizes information hierarchically to ease network use and management.

In addition, Active Directory manages the relationships among objects and containers to provide a single, centralized, comprehensive view. This makes resources easier to find, manage, and use in a highly distributed network. The Active Directory hierarchy is flexible and configurable, so organizations can organize resources in a way that optimizes their usability and manageability.

In Figure 1 above, containers are used to represent collections of users, machines, devices, and applications. Containers can be nested (created one-inside-the-other) to reflect accurately the company's organizational structure. In this case, marketing and personnel organization containers represent those respective departments, and their relationship to one another, within the company. Grouping objects in the directory lets administrators manage objects on a macro-level (as collections) rather than one-by-one. This increases management efficiency and accuracy while letting organizations align network management with their business processes.

Object-oriented Storage

As mentioned earlier, Active Directory stores information about network elements in the form of objects. These objects can be assigned attributes, which describe specific characteristics about the object. This lets companies store a wide range of information in the directory and tightly control access to it.

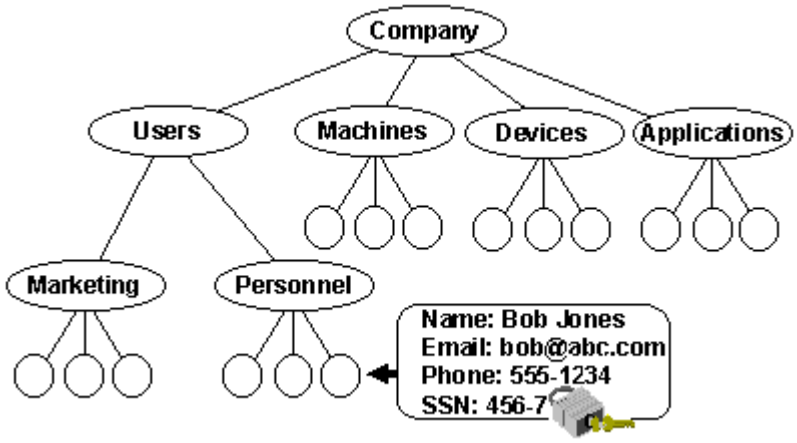


Figure 2: Active Directory objects and attributes are protected by access control lists.

As illustrated in Figure 2 above, object- and attribute-level security lets administrators precisely control access to information stored in the directory. For example, a user object stored in the directory for Bob Jones has attributes for Bob's name, e-mail address, phone number, and Social Security number. The Active Directory lets administrators assign access privileges for each attribute of the object, as well as for the entire object. In this case, the system administrator has allowed global access to the Bob Jones object, but has locked access of the Social Security Number attribute.

Multi-Master Replication

To provide high performance, availability, and flexibility in distributed

environments, the Active Directory uses multi-master replication. As illustrated in Figure 3 below, this lets organizations create multiple copies of the directory, known as directory replicas, and place them throughout the network. Changes made anywhere on the network are automatically replicated throughout the network. (This is in contrast to single-master replication in which all changes must be made to a single, authoritative directory replica).

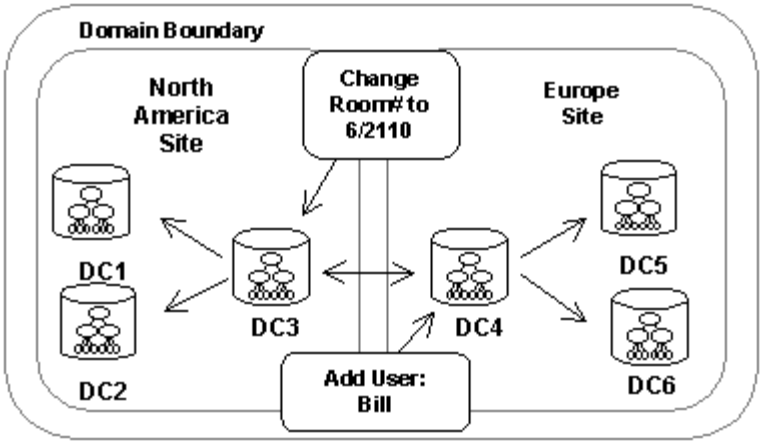


Figure 3: Active Directory supports multi-master replication for flexibility, high-availability, and performance.

For example, fully synchronized directory replicas can be made available to each location in a wide area network (WAN). Such a process can give users faster performance because they can locate resources using the local directory service rather than by traversing the WAN. These same directories could be managed locally or remotely depending on available administrative resources.

Totally integrated with Windows 2000 Server, Active Directory gives network administrators, developers, and users access to a directory service that:

- Simplifies management tasks.
- Strengthens network security.
- Makes use of existing systems through interoperability.

Simplifies Management

Distributed systems often lead to time-consuming and redundant management. As companies add applications to their infrastructure and hire more personnel, they need to distribute software to the desktop

appropriately and manage multiple application directories. Active Directory allows companies to significantly lower management costs by providing a single place to manage users, groups and network resources, as well as distribute software and manage desktop configurations. For example, Active Directory uses one place for managing both Windows 2000 users and Microsoft Exchange mailbox information. Active Directory helps companies simplify management because it:

- **Eliminates redundant management tasks.** Provides a single-point of management for Windows user accounts, clients, servers, and applications as well as the ability to synchronize with existing directories.
- **Reduces trips to the desktop.** Automatically distributes software to users based on their role in the company, reducing or eliminating multiple trips that system administrators need to make for software installation and configuration.
- **Better maximizes IT resources.** Securely delegates administrative functions to all levels of an organization.
- **Lowers total cost of ownership (TCO).** Simplifies the management and use of file and print services by making network resources easier to find, configure, and use.

How Active Directory Simplifies Management

By organizing users and network resources hierarchically, Active Directory lets administrators have a single point of management for user accounts, clients, servers, and applications. This reduces redundant management tasks and increases accuracy by letting administrators manage containers or groups of objects rather than each object individually.

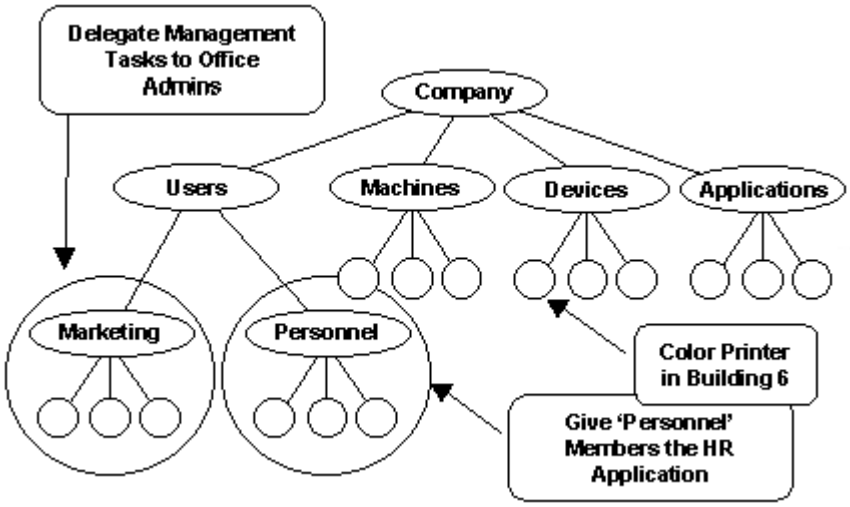


Figure 4: Active Directory simplifies management of network resources.

Active Directory lets administrators delegate specific administrative privileges and tasks to individual users and groups to make better use of system administration resources. As shown in Figure 4 above, specific management tasks, such as resetting user passwords, can be delegated to the office administrators in the marketing organization. More privileged functions, such as “create user,” can be reserved for IT administrators.

Active Directory also lets organizations automatically distribute software to users based on their role in the company. For example, a company could specify that all users in the personnel container have the HR application available to them regardless of where they log on to the network. Active Directory stores this information centrally and works with IntelliMirror™ management technologies to install assigned applications automatically and give users the ability to access their own desktops regardless of the workstation they use in the network.

In addition to making network management easier for administrators, Active Directory also makes it easier for everyone to use the network. For example, users can directly query the directory for network resources such as printers. Since the directory can store attributes about objects, it can store the location and the capabilities of an organization's printers and expose these attributes as search criteria — so the user can search for "printers in Building 6 that print color" directly from the "Start" menu in Windows. What’s more, the directory can refer the desktop operating system to all the configuration information it needs to set up a new printer–-so when users find the printer they want, they can use it right away.

Strengthens Security

Strong and consistent security services are essential to corporate networks. Managing user authentication and access control is often tedious and prone to error. Active Directory centralizes management and enforces role-based security consistent with an organization's business processes. For example, support for multiple authentication protocols such as Kerberos, X.509 certificates, and smart cards — combined with a flexible access control model — enables powerful and consistent security services for internal desktop users, remote dial-up users, and external e-commerce customers. The following are some ways in which Active Directory strengthens security:

- **It improves password security and management.** By providing single sign-on to network resources with integrated, high-powered security services that are transparent to end users.
- **It ensures desktop functionality.** By locking-down desktop configurations and preventing access to specific client machine

operations, such as software installation or registry editing, based on the role of the end user.

- **It speeds e-business deployment.** By providing built-in support for secure Internet-standard protocols and authentication mechanisms such as Kerberos, public key infrastructure (PKI) and lightweight directory access protocol (LDAP) over secure sockets layer (SSL).
- **It tightly controls security.** By setting access control privileges on directory objects and the individual data elements that make them up.

How Active Directory Strengthens Security

One of the most important architectural advantages of Windows 2000 Server is the integration of Active Directory and its advanced security features that enable a new level of data protection. This is particularly important for organizations that do business over the Internet.

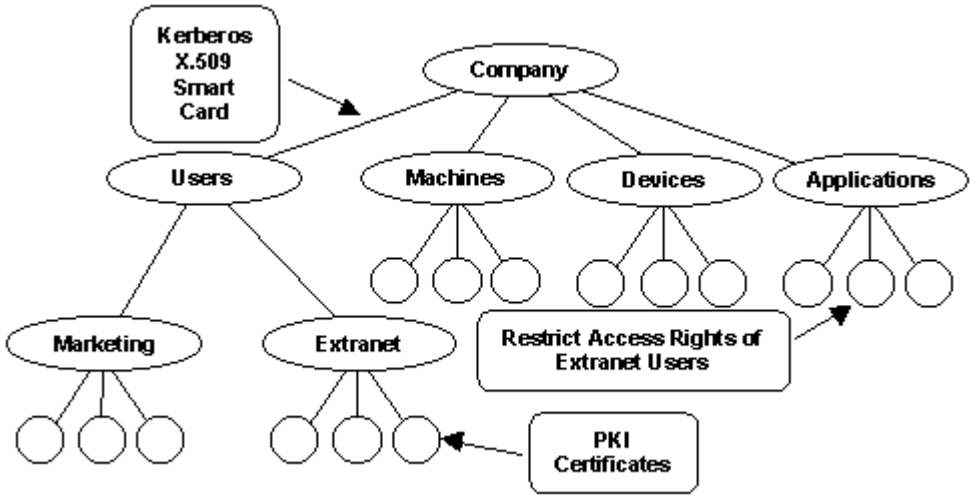


Figure 5: Active Directory provides Internet-ready security services to protect data while facilitating access.

As illustrated in Figure 5 above, Active Directory acts as the central authority for governing authentication of user identity and controlling access to network resources. It supports a number of authentication mechanisms used to prove identity upon logon to Windows 2000, including Kerberos, x.509 certificates, and smart cards. Once a user is authenticated and logged on, all resources in the system are protected and access is granted or denied based on a single authorization model. This means that organizations don't have to protect resources one way for users who logon via the intranet and another way for those who use digital certificates to access resources over the Internet.

In addition, Active Directory natively supports a fully integrated public

key infrastructure and Internet secure protocols, such as LDAP over SSL, to let organizations securely extend selected directory information beyond their firewall to extranet users and e-commerce customers. In this way, Active Directory strengthens security and speeds deployment of e-business by letting administrators use the same tools and processes to manage access control and user privileges across internal desktop users, remote dial-up users, and external e-commerce customers.

Extends Interoperability

Many companies have a diverse collection of technologies that must work together. As a result, many corporate networks have an equally diverse collection of disparate directories as part of e-mail servers, applications, network devices, firewalls, e-commerce applications, and more. Active Directory provides a set of standard interfaces for application integration and open synchronization mechanisms to ensure that Windows can interoperate with a wide variety of applications and devices. Active Directory extends interoperability because it:

- Takes advantage of existing investments and ensures flexibility. Standards-based interfaces to all features make use of investments and ensure flexibility for future applications and infrastructure.
- Consolidates management of multiple application directories. Using open interfaces, connectors, and synchronization mechanisms, organizations can consolidate directories including Novell's NDS, LDAP, ERP, e-mail, and other mission-critical applications.
- Allows organizations to deploy directory-enabled networking. Network devices from leading vendors such as Cisco and 3COM can use the directory to let administrators assign quality of service and allocate network bandwidth to users based on their role in the company.
- Allows organizations to develop and deploy directory-enabled applications. Using the fully extensible directory architecture, developers can build applications that deliver functionality tailored to the needs of the end user.

How Active Directory Extends Interoperability

Active Directory provides a central integration point for bringing diverse systems together and for consolidating directories and management tasks. It does this by exposing all of the Windows 2000 directory features through standards-based interfaces such as LDAP, ADSI, JADSI, and MAPI so companies can consolidate existing directories and develop directory-enabled applications and infrastructure. One example of how Microsoft is using Active Directory in its own product-line is Microsoft Exchange. The Exchange server has been integrated with Active Directory to enable companies to manage Windows 2000 user accounts and Exchange mailboxes in one place.

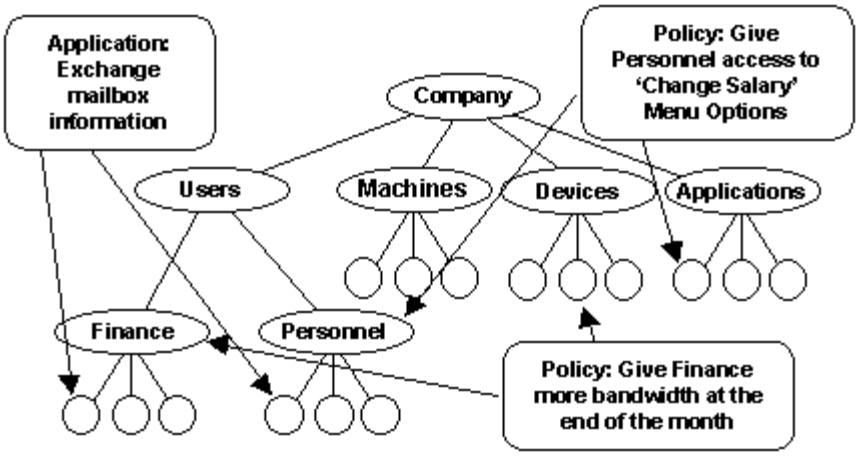


Figure 6: Active Directory provides a platform for integrating and extending systems through open interfaces, connectors, and synchronization mechanisms.

As shown in Figure 6 above, Active Directory also provides a development platform for directory-enabled applications. This lets application developers control the behavior of an application based on the user's role in the company. For example, a directory-enabled application could reference a user's profile in the directory and provide specific menu items and functionality based on his or her job function. That way, a user in personnel could see the "Change Salary" menu item in an HR application, while a user in finance would not see that menu, even if the two users share a computer.

Just as organizations can improve the way their directory service and applications work together, so can they improve the way their network hardware and software work with their directory service. By providing a platform for directory-enabled networks, Active Directory lets companies match network resource allocation to their business-process requirements. In particular, administrators can allocate network bandwidth to users based on their business needs. For example, an administrator could create a policy that ensures that users in the finance department are allocated additional bandwidth when they are busy closing books at the end of the month.

The benefits of Active Directory can be extended beyond the Windows environment. The open synchronization mechanisms within Active Directory ensure interoperability of the Windows platform with a wide variety of applications and devices. For example, native support for LDAP, DirSync, and ADSI interfaces enables leading vendors such as Cisco, SAP, BAAN, and 3COM to integrate with Active Directory to provide simplified and powerful management of their multi-platform products.

Today, information about people, applications, and resources is scattered

throughout most corporate information systems — and is continuing to proliferate. Networks have evolved from loose collections of connected devices to complex ecosystems made up of interdependent resources. As a result, network operating systems need to provide much more than simple network file and print services. They now need to transparently manage the relationships between distributed network resources.

The Active Directory service within Windows 2000 Server provide a focal point for managing and securing Windows user accounts, clients, servers, and applications. In addition, Active Directory is designed to integrate with the non-Windows directories within existing systems, applications, and devices to provide a single place and a consistent way of managing an entire network infrastructure. In this way, Active Directory increases the value of an organization's existing investments and lowers the overall costs of computing by reducing the number of places where administrators need to manage directory information.